UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF GEORGIA

SAVANNAH DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	Case No. CR414-348
	)	
ALEJANDRO TORRES	)	

REPORT AND RECOMMENDATION

Defendant, charged with the receipt, distribution, and possession of child pornography, has moved to suppress all evidence seized from his residence and personal computer pursuant to a search warrant issued by this Court. As his "primary" ground for suppression, defendant contends that state agents "illegally obtained" a subpoena authorizing Comcast Communication to divulge the name and physical address for the subscriber of an Internet Protocol ("IP") address that had offered a large number of child pornography images for downloading. Doc. 40 at 3. Because the subscriber information from Comcast "was compelled by unlawful means," *id.* at 26, and because that information was central to the probable cause basis for the search warrant, defendant contends that

the search "infringed his constitutionally protected privacy interests." *Id.* at 12.

I. BACKGROUND

On August 1, 2014, an FBI agent applied for a warrant to search 1110 Montgomery Street, Apartment B, Savannah, Georgia and to seize images of child pornography stored on any computer at that residence. Doc. 31-1 at 1, 3. The 20-page affidavit presented in support of the warrant related that Liberty County, Georgia Detective Charles Woodall, a member of the Southeast Georgia Child Exploitation Task Force (SEGCETF), had observed that a computer operating on IP address 98.244.189.89 was offering large numbers of suspected child pornography files for distribution.[1] *Id.* at 2, 15. From July 8 through July 27, 2014, Detective Woodall downloaded some 38 files that contained images of children (some believed to be 3 or 4 years old) engaged in sexually explicit activity. *Id.* at 15-21. Woodall determined that the unknown computer user under investigation had made some 80 to 100 different

[1] Detective Woodall connected to this computer using the publicly-available Ares peer-to-peer ("P2P") file sharing network. *Id.* at 15. "Ares is a program which is free to download and [is] used to exchange files between computer users." *Id.* ¶ 23; *see id.* at 9 ¶ 6; *id.* at 12-13 ¶ 15.

child pornography files available for download during that time frame. *Id.* at 19 ¶ 41.

The affidavit further related that another SEGCETF member, Det. Joe Heath, had also downloaded files from that same IP address. Doc. 31-1 at 19 ¶ 33. One of the detectives (apparently Heath) then "submitted a subpoena which he served on Comcast Communication." *Id.* Pursuant to that subpoena, Comcast identified the subscriber for the IP address as Zachary Herrmann and furnished the subscriber's physical address. *Id.* at 19 ¶ 34.

During the execution of the search warrant issued for that residence, the agents spoke to defendant Torres, who admitted that he, not the Comcast subscriber, was the person who had been downloading child pornography. Doc. 31-2 (arrest warrant affidavit) at 4, ¶ 13. Defendant indicated that all of the images and videos he had downloaded were stored on a laptop computer that he had owned for many years and that was located in his bedroom. *Id.* ¶ 14. After seizing and searching that computer, agents confirmed that it contained child pornography.

II. ANALYSIS

Again, defendant's primary claim is that the subpoena used by state agents to obtain the subscriber information for IP address 98.244.189.89 was "illegally obtained." The government contends that defendant has no "standing" to object to the acquisition of the subscriber information from Comcast, because whether the acquisition of that information was proper or not, "no privacy interest of his own was violated." Doc. 42 at 2.

"Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted." *Alderman v. United States*, 394 U.S. 165, 174 (1969). The test for whether a defendant's personal rights are violated depends on "whether the disputed search and seizure . . . infringed an interest of the defendant which the Fourth Amendment was designed to protect." *Rakas v. Illinois*, 439 U.S. 128, 140 (1978). For nearly half a century, the Supreme Court has held that a defendant must assert a *legitimate* expectation of privacy -- "'one that society is prepared to recognize as reasonable'" -- in order to claim the protections of the Fourth Amendment. *Smith v. Maryland*, 442 U.S. 735, 740 (1979). "What a

person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz v. United States*, 389 U.S. 347, 351 (1967).

In reliance on *Katz*, the Supreme Court held in *Smith v. Maryland* that the warrantless installation of a pen register (on telephone company property) to record the telephone numbers dialed from a suspect's residence did not constitute a "search" with the meaning of the Fourth Amendment. *Id.* at 742. "[A] person has "no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44. Because the user of a telephone voluntarily conveys information about the numbers he dials to the phone company, he can claim no Fourth Amendment privacy protection in that information and assumes the risk of its disclosure to the government. [2]

The *Smith* analysis applies here and defeats defendant's privacy claim as to the subscriber information Comcast disclosed to the state

---

[2] The Court cited *United States v. Miller*, 425 U.S. 435, 442-44 (1976), which held that a bank depositor has no legitimate expectation of privacy in the information that he conveys to the bank and its employees: "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government . . . *even if* the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party [bank] will not be betrayed." *Id.* at 443 (emphasis added).

agents. "Every federal court to address this issue has held that subscriber information provided to an Internet Provider is not protected by the Fourth Amendment's privacy expectation." *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (collecting cases); *United States v. Wheelock*, 772 F.3d 825, 828-29 (8th Cir. 2014) (Fourth Amendment did not prohibit Comcast from conveying subscriber information to government authorities, as defendant had no reasonable expectation of privacy in the information he revealed to a third party); *United States v. Cray*, 673 F. Supp. 2d 1368, 1375 (S.D. Ga. 2009) (defendant had no legitimate privacy interest in subscriber information he furnished to his Internet provider).[3] Thus, none of defendant's *constitutionally* guaranteed privacy rights were violated when Comcast disclosed to state agents the subscriber information for an IP address known to be trafficking in child pornography. And since it is undisputed that defendant was not even the subscriber on the Comcast account (and

[3] Indeed, it is unclear whether even *the contents* of emails stored on an Internet Service Provider's ("ISP") servers are entitled to Fourth Amendment protection. *Rehberg v. Paulk*, 611 F.3d 828, 843-47 (11th Cir. 2010) (defendant law enforcement officials were entitled to qualified immunity on § 1983 claim that they violated plaintiff's constitutional rights by issuing a subpoena to his ISP and obtaining emails sent from his personal computer, as the law was not clearly established that plaintiff had a reasonable expectation of privacy in the contents of emails sent voluntarily over the global Internet and stored on a third-party ISP's server).

therefore had no privity of contract with that company), he cannot reasonably claim even a *subjective*, much less a legitimate, expectation of privacy in the name and physical address of the Comcast account holder.[4]

Defendant (understandably) spends little time discussing Fourth Amendment principles but instead focuses his argument on the state agents' failure to comply with a state statute governing the issuance of subpoenas.[5] Specifically, defendant claims that the state agents lacked the authority to issue an administrative subpoena, as it was not approved by the appropriate GBI officials or the state Attorney General, and that the subpoena was not issued pursuant to a "court order," as it was signed

---

[4] Defendant initially claimed a violation of the "Fourth Amendment right to privacy of *his* confidential information possessed by Comcast communications pursuant to its contract *with Movant*." Doc. 31 at 3 (emphasis added). This assertion is not supported by the arrest warrant affidavit attached to defendant's brief. Doc. 31-2 at 3, ¶ 11 (Comcast identified the subscriber as Zachary Herrmann). Moreover, at the evidentiary hearing defendant did not dispute the government's assertion that it was defendant's roommate, *not* defendant, who had a contractual relationship with Comcast, and neither of defendant's post-hearing briefs reasserts the initial claim that any of *his* confidential information was disclosed to the state agents.

[5] Defendant cites O.C.G.A. § 35-3-4.1, which authorizes certain officials of the Georgia Bureau of Investigation to issue an administrative subpoena seeking basic subscriber information (but not the contents of communications) for any computer used in furtherance of child pornography or other offenses against minors. But rather than using an administrative subpoena, the state agents in this case sought and obtained a subpoena from the Effingham County Superior Court. Although that subpoena was signed only by a deputy clerk and does not reference any statutory provision as authority for its issuance, Comcast nevertheless divulged the subscriber information sought by the subpoena.

only by a clerk of court, not a judge. Defendant then reasons that without the "unlawfully obtained" information from Comcast regarding the physical location of the IP address under investigation, the search warrant affidavit fails to establish probable cause for the search of his residence. Doc. 31 at 4.

Undergirding defendant's argument is the unstated but implicit assumption that the judicially-crafted exclusionary rule -- designed to remedy violations of a defendant's *constitutional* rights -- applies to information gained in violation of state statutory provisions pertaining to the issuance of subpoenas. But as the Eighth Circuit recently held, a law enforcement officer's failure to comply with a state statute authorizing an administrative subpoena for subscriber information of an IP address used to distribute child pornography "would not warrant suppression of the evidence gained because federal courts in a federal prosecution do not suppress evidence that is seized by state officers in violation of state law, so long as the search complied with the Fourth Amendment." *Wheelock*, 772 F.3d at 830; *see also* 1 Wayne R. LaFave, *Search and Seizure* § 1.5(c) at 228-30 (5th ed 2012) ("if either federal or state officers conduct a search that is illegal under the law of the state where undertaken, the

fruits thereof are not constitutionally barred from evidence in the federal courts.").[6] Because the acquisition of the subscriber information from Comcast violated none of defendant's Fourth Amendment rights, the agents' alleged noncompliance with the technical requirements of the Georgia subpoena statutes does not warrant the application of the exclusionary rule. Defendant, therefore, is not entitled to an evidentiary hearing to determine whether the state agents complied with state law in obtaining a subpoena directing the disclosure of his *roommate's* subscriber information.[7]

---

[6] The federal statute requiring Internet providers to furnish basic subscriber information in response to an administrative subpoena "authorized by a Federal or State statute," or a court order from a federal or state court of competent jurisdiction, 18 U.S.C. § 2703(c), (d), provides a civil action for damages as the *exclusive* remedy "for non-constitutional violations of this chapter." 18 U.S.C. § 2708. *See also Cray*, 673 F. Supp. 2d at 1376 (the violation of a federal statute will not result in the suppression unless the statute itself specifies exclusion as a remedy).

[7] Defendant seeks a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), which requires that a defendant make "a substantial preliminary showing" that a warrant affidavit contains a false statement and establish that the affiant inserted the falsehood deliberately or with reckless disregard for the truth. *Id.* at 155-56, 171-72. Defendant has not pointed to *any* false statement in the warrant affidavit. The only passage he references is the FBI agent's averment that a state agent "submitted a subpoena which he served on Comcast Communication." Doc. 31-1 at 19, ¶ 33. But this is undisputably a *true* statement: a state agent *did* seek and obtain a subpoena which he served on Comcast. Defendant simply contends that the state agent did not comply with state statutory procedures in obtaining that subpoena. Nor has defendant made any "offer of proof," *Franks*, 438 U.S. at 171, that the FBI agent knew that the state agents failed to comply with state law in securing their subpoena, had any basis for doubting the authenticity of the subpoena, acted unreasonably in failing to research state subpoena law before relying on the state agents'

Defendant has thus shown no basis for the excision of the subscriber information from the search warrant affidavit. His alternative claim that, even with this information, the affidavit is "facially insufficient" is frivolous. Doc. 31 at 2. Using a publicly available peer-to-peer file sharing network, agents accessed and downloaded numerous images of child pornography offered for distribution by a computer operating at a particular IP address. They then determined, using other publicly available information, that this IP address was registered to Comcast Cable Communications. Presented with a subpoena (the validity of which is immaterial to this analysis), Comcast disclosed that the subscriber resided at a particular Savannah, Georgia address. That the affidavit furnished a sufficient probable cause basis for the issuance of a search warrant for that residence is beyond debate. The search of defendant's residence and computer was conducted pursuant to lawful warrant issued by this Court, and he has offered no basis for the suppression of the evidence seized pursuant to that warrant. And because defendant's statements to the agents during

---

representations, or thought that Comcast's disclosure of the subscriber information pursuant to a defective state subpoena would have precluded this Court from relying on that information (it would not have!).

the execution of the search warrant were not the tainted fruit of an illegal search, those statements are admissible at his trial.

Defendant's motion to suppress is without merit and should be **DENIED**.

SO REPORTED AND RECOMMENDED this 14th day of January, 2015.

UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF GEORGIA